

WHAT IS CLAIMED IS

1 1. A security mechanism for enabling a user to commence a session between
2 a network peripheral device and a network, comprising:
3 an immutable memory element that contains first information including
4 application software that initiates that provides security services;
5 a persistent memory element that contains second information to enable the
6 security mechanism to configure the network peripheral device to different networks;
7 a volatile memory element that contains third information, including the critical
8 data for authentication, said third information erased from the volatile memory at the
9 completion of each connection session; and
10 a tamper-evident enclosure for enclosing the memory elements.

1 2. The apparatus according to claim 1 wherein the security services include
2 authentication of the security mechanism itself and authentication of the user to the
3 network upon receipt of identification information from the security mechanism and the
4 user, respectively.

1 3. The security mechanism according to claim 1 wherein the immutable
2 memory contains a private key for encrypting the user and security mechanism
3 identification information.

1 4. The security mechanism according to claim 1 wherein the immutable
2 memory comprises a Read-Only Memory (ROM).

1 5. The security mechanism according to claim 4 wherein the immutable
2 memory further includes a Write-once ROM.

1 6. The security mechanism according to claim 1 wherein the persistent
2 memory comprises at least one of one of a CMOS Random Access Memory (RAM) and
3 a Programmable Read Only Memory (PROM).

1 7. The security mechanism according to claim 1 wherein the volatile memory
2 comprises a random access memory.

1 8. The security mechanism according to claim 1 wherein the tamper evident
2 enclosure readily exhibits any attempt to gain access there through to the memory
3 elements enclosed therein.

1 9. The security mechanism according to claim 1 wherein the physical
2 security of the security mechanism depends on the degree of tamper resistance of the
3 enclosure.

1 10. A method for facilitating a secure connection session with a user between
2 a network peripheral device and a network, comprising the steps of:
3 accessing an immutable memory element that contains first information that
4 provides security services;
5 accessing a persistent memory element that contains second information including
6 configuration information to enable the security mechanism to configure the network
7 peripheral device to the network;
8 accessing a volatile memory element that contains third information, including
9 critical data for authentication; and
10 erasing said third information not later than the end of the connection session so
11 no third information remains in the volatile memory between sessions.

1 11. The method according to claim 10 wherein the security services include
2 authentication of the security mechanism itself and authentication of the user to the
3 network upon receipt of identification information from the security mechanism and the
4 user, respectively.